Cybercrime, electronic evidence and the rule of law in cyberspace

Santiago de Chile, 21 March 2017

Alexander Seger
Executive Secretary
Cybercrime Convention Committee
Council of Europe
Strasbourg, France
alexander.seger@coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

www.coe.int/cybercrime

1

Cybercrime and electronic evidence: challenges

Offences against and by means of computers (Cybercrime)

- Attacks against core values of democratic societies

+

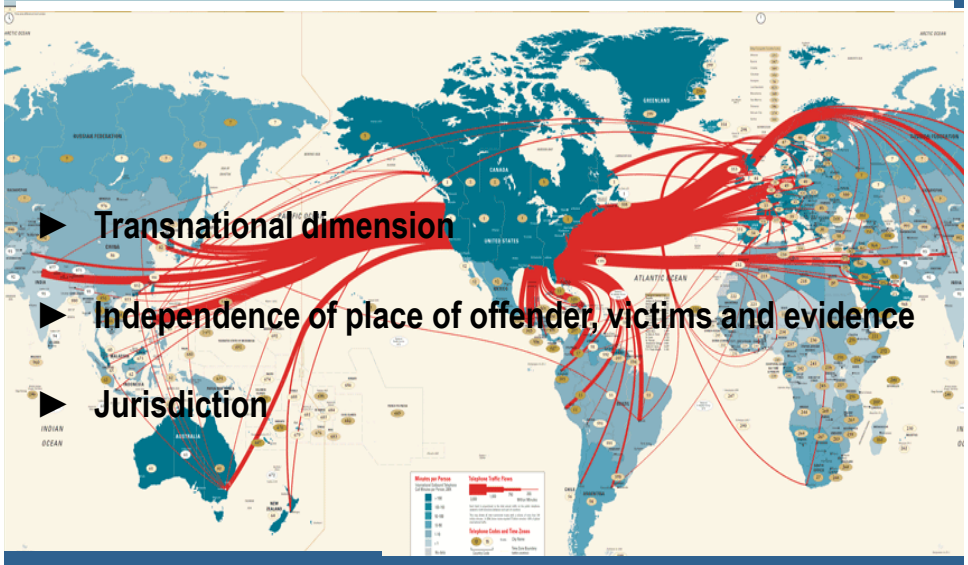
Evidence in relation to any crime stored on computer systems or storage devices

- Often "somewhere" in the cloud)

2

3

Crime scene in cyberspace



- Transnational dimension
- Independence of place of offender, victims and evidence
- Jurisdiction

4

Cybercrime and electronic evidence: Challenges for criminal justice

- The scale and quantity of cybercrime, devices, users and victims
- Technical challenges (VPN, anonymisers, encryption, VOIP, NATs etc.)
- Cloud computing, territoriality and jurisdiction
  - Cloud computing: distributed systems ▶ distributed data ▶ distributed evidence
  - Unclear where data is stored and/or which legal regime applies
  - Service provider under different layers of jurisdiction
  - Unclear which provider for which services controls which data
  - Is data stored or in transit ▶ production orders, search/seizure or interception?
- The challenge of mutual legal assistance
- No data ▶ no evidence ▶ no justice

5

Cybercrime and the rule of law in cyberspace

Cybercrime = ?

↓

Reported to/recorded by police = 100

↓

Investigated

↓

Prosecuted

↓

Adjudicated = 1 or 0.1 or 0.01?

↓

= Cyberspace basically safe, crime the exception, offenders brought to justice, individuals and their rights protected?
= Rule of law in cyberspace?
= Do governments meet obligation to protect individuals against crime?

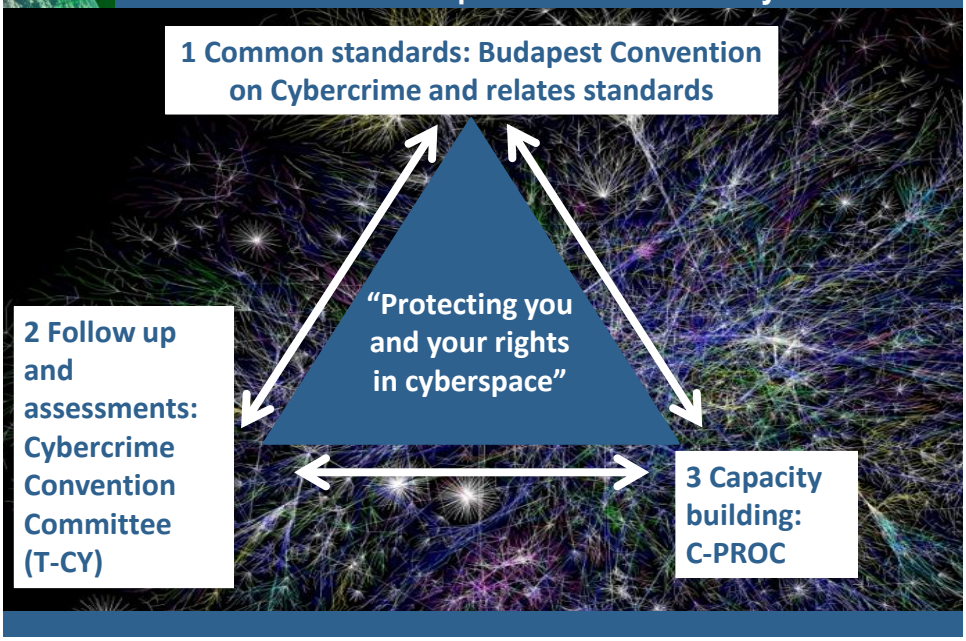
6

Cybercrime and electronic evidence: Solutions?

- How to ensure the rule of law in cyberspace?
- And how to reconcile the need for efficient law enforcement and access to data with human rights and rule of law requirements?

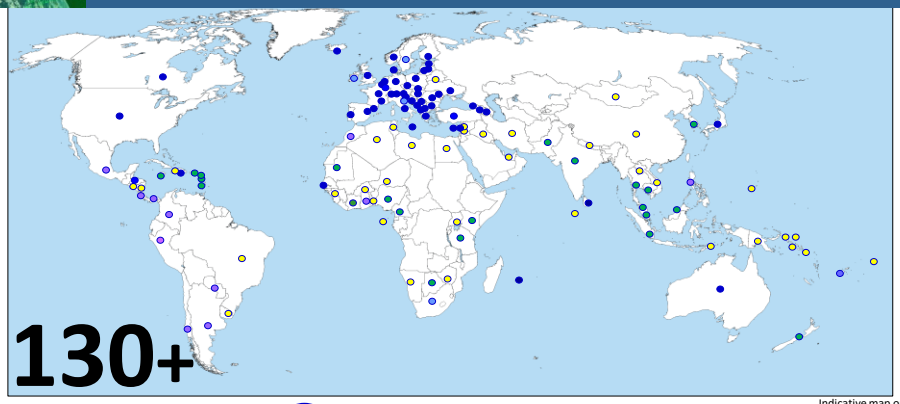
7

Strengthening the rule of law in cyberspace: The framework of the Budapest Convention on Cybercrime



8

Reach of the Budapest Convention as a guideline



Budapest Convention
Ratified/acceded: 53
Signed: 5
Invited to accede: 10
= 68

Other States with laws/draft laws largely in line with Budapest Convention = 20

Further States drawing on Budapest Convention for legislation = 45+

9

OAS Member States and the Budapest Convention

Parties:

- Canada
- Dominican Republic
- Panama
- USA

Invited to accede:

- Argentina
- Chile
- Colombia
- Costa Rica
- Mexico
- Paraguay
- Peru

10

Adopt legislation in line with the Budapest Convention

Criminalising conduct
- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Fraud and forgery
- Child pornography
- IPR-offences

+

Procedural tools
- Expedited preservation
- Search and seizure
- Interception of computer data
- + Safeguards!

+

International cooperation
- Extradition
- MLA
- Spontaneous information
- Expedited preservation
- MLA for accessing computer data
- MLA for interception
- 24/7 points of contact

Harmonisation

11

Participate in Cybercrime Convention Committee (T-CY)

Established under Article 46 Budapest Convention

Membership
(status December 2016):

- 53 Members (State Parties)
- 15 Observer States
- 10 International organisations (African Union Commission, Commonwealth Sec, ENISA, European Union, Europol, INTERPOL, ITU, OAS, OECD, OSCE, UNODC)

Functions:

- Assessments of the implementation of the Convention by the Parties
- Guidance Notes
- Draft legal instruments
- Etc.

2 x plenaries per year
+ Bureau and Working Group meetings

12

T-CY Guidance Notes

Guidance Notes adopted:

- ✓ Notion of "Computer Systems"
- ✓ Botnets
- ✓ Identity theft
- ✓ DDOS attacks
- ✓ Critical Infrastructure Attacks
- ✓ Malware
- ✓ Transborder access to data (Article 32)
- ✓ Terrorism
- ✓ Production orders for subscriber information (Article 18)

13

Crime and jurisdiction in cyberspace ► solutions proposed under the Budapest Convention on Cybercrime

Context:

Budapest Convention on Cybercrime ► Cybercrime Convention Committee (T-CY) ► Cloud Evidence Group ► Recommendations September 2016 ► now under consideration by T-CY

Rationale:

- Cybercrime AND electronic evidence in relation to any crime
- E-evidence on servers in foreign, unknown, multiple or shifting jurisdictions, in the cloud
- No data, no evidence, no prosecution, no justice, no rule of law (in cyberspace)

Issues:

- Differentiating subscriber versus traffic versus content data
- Limited effectiveness of MLA
- Loss of location and transborder access jungle
- Provider present or offering a service in the territory of a Party
- Voluntary disclosure by US-providers
- Emergency procedures
- Data protection

Solutions:

1. More efficient MLA
2. Guidance Note on Article 18
3. Domestic rules on production orders (Article 18)
4. Cooperation with providers: practical measures
5. Protocol to Budapest Convention

www.coe.int/cybercrime

14

Current practice: "Voluntary" disclosure by private sector entities

	Requests for data sent to Apple, Facebook, Google, Microsoft, Twitter and Yahoo in 2015		
Parties	Received	Disclosure	%
Australia	6 777	4 580	47%
Belgium	1 992	1 453	68%
Bulgaria	8	2	25%
Canada	1 157	884	76%
Finland	227	172	76%
France	27 213	14 746	54%
Germany	29 092	15 469	53%
Japan	2 018	1 112	55%
Netherlands	1 605	1 213	76%
Portugal	3 255	1 751	54%
Romania	76	30	39%
United Kingdom	29 937	21 075	70%
USA	89 350	70 116	78%
Total excluding USA	**138 612**	**82 529**	**60%**
Total including USA	227 962	152 644	67%

15

Solution 2: Guidance Note on Article 18

Guidance Note on Article 18 Budapest Convention on production of subscriber information:

- **Domestic production orders for subscriber information if a provider is in the territory of a Party even if data is stored in another jurisdiction (Article 18.1.a)**
- **Domestic production orders for subscriber information if a provider is NOT necessarily in the territory of a Party but is offering a service in the territory of the Party (Article 18.1.b)**

Agreed by T-CY on 28 Feb 2017

www.coe.int/cybercrime

16

Solution 5: Protocol to Budapest Convention

A. Provisions for more efficient MLA

B. Provisions for direct cooperation with providers in other jurisdictions

C. Framework and safeguards for existing practices of transborder access to data

D. Data protection

Need for Protocol agreed by T-CY in principle in Nov 2016.
TOR to be agreed upon in June 2017

Participate in capacity building programmes

Capacity building on cybercrime electronic evidence

Multiple programmes:

- Legislation
- Specialised law enforcement units
- Training of prosecutors and judges
- Public/private cooperation
- Targeting proceeds from crime online
- International cooperation

- Dedicated Cybercrime Programme Office of the Council of Europe (C-PROC) in Bucharest, Romania
- Cooperation with OAS and other organisations

- Priority to countries committed to implement Budapest Convention
- Support to any country regarding legislation

Current capacity building programmes

- **GLACY+** EU/COE Joint Project on Global Action on Cybercrime Extended
- **Cybercrime@EAP II** EU/COE Eastern Partnership on international cooperation
- **Cybercrime@EAP III** EU/COE Eastern Partnership on public/private cooperation
- **iPROCEEDS** Cooperation on Cybercrime: targeting proceeds from online crime
- **Cybercrime@Octopus** (voluntary contribution funded)

In preparation

- **CyberSouth** EU/COE project for the Southern Neighbourhood

19

Capacity building activities: snapshot 6 – 17 March 2017

- 6-7 March, Bucharest – Project planning workshop CyberSouth (Cybercrime@Octopus)
- 6-9 March, Yerevan, Armenia – Training of investigators, prosecutors and judiciary in international cooperation on electronic evidence/multinational providers cooperation (EAP II/III)
- 13 – 16 March, Tirana, Albania – Guidelines on detection of crime proceeds online and regional workshop on interagency cooperation (iPROCEEDS)
- 13-16 March, Baku, Azerbaijan – Training of investigators, prosecutors and judiciary in international cooperation on electronic evidence/multinational provider cooperation (EAP II/III)
- 13-17 March, Colombo, Sri Lanka – Development of Cybercrime investigations, digital forensic capabilities (INTERPOL) combined with in-country workshops and advice on interagency cooperation (INTERPOL) and private public partnerships to fight cybercrime (INTERPOL) (GLACY+)
- 13-17 March, Dakar, Senegal – Support regional judicial ToT on cybercrime an e-evidence, GLACY+

20

Benefits of Budapest Convention

- ✓ Coherent legal framework that meets rule of law requirements
- ✓ Trusted and efficient cooperation with other Parties
- ✓ Participation in the Cybercrime Convention Committee (T-CY)
- ✓ Participation in future standard setting (Guidance Notes, Protocols and other additions to Budapest Convention)
- ✓ Enhanced trust by private sector
- ✓ Capacity building

"Cost": Commitment to cooperate

Disadvantages?

21